

(19) RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

(11) N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 692 701

(21) N° d'enregistrement national :

92 07430

(51) Int Cl⁵ : G 06 F 15/46

(12)

DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 18.06.92.

(30) Priorité :

(71) Demandeur(s) : AEROSPATIALE Société Nationale Industrielle — FR.

(72) Inventeur(s) : Cavasa Victor et Schuster Patrick.

(43) Date de la mise à disposition du public de la demande : 24.12.93 Bulletin 93/51.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule.*

(60) Références à d'autres documents nationaux apparentés :

(73) Titulaire(s) :

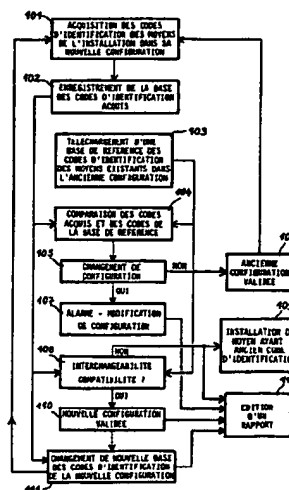
(74) Mandataire : Brevatome.

(54) Procédé de contrôle de configuration d'une installation complexe et dispositif pour la mise en œuvre de ce procédé.

(57) L'invention concerne un procédé de contrôle de configuration d'une installation complexe, ainsi qu'un dispositif mettant en œuvre ce procédé.

Le procédé consiste essentiellement à :

- enregistrer (102) dans une mémoire d'un ordinateur de l'installation, une base des codes d'identification des moyens de l'installation, y compris le code d'identification du nouveau moyen, pour obtenir une base de la nouvelle configuration de l'installation,
- enregistrer (103) dans la mémoire dudit ordinateur une base de référence des codes d'identification des moyens de l'installation, avant ledit remplacement, cette base correspondant à la configuration, dite ancienne, de l'installation,
- comparer (104) la base de référence des codes d'identification de l'ancienne configuration avec la base des codes d'identification de la nouvelle configuration, pour déclencher (107) une alarme lorsque la comparaison indique une modification de configuration.



FR 2 692 701 - A1



PROCEDE DE CONTROLE DE CONFIGURATION D'UNE INSTALLATION
COMPLEXE ET DISPOSITIF POUR LA MISE EN
OEUVRE DE CE PROCEDE

5

DESCRIPTION

La présente invention concerne un procédé
de contrôle de configuration d'une installation
complexe, ainsi qu'un dispositif de mise en oeuvre
10 de ce procédé.

Ce procédé et ce dispositif sont applicables
aux installations complexes, de configuration déterminée
ou évolutive. Ces installations comprennent généralement
des moyens combinés tels que des capteurs, des systèmes
15 de traitement incluant des calculateurs commandant
par exemple des asservissements et d'une manière
générale des moyens combinés interagissant les uns
avec les autres pour obtenir un résultat souhaité..

La configuration d'une installation est
20 déterminée par les concepteurs de celle-ci. Cette
configuration définit notamment l'organisation des
différents moyens fonctionnels qui composent
l'installation, les spécifications fonctionnelles
essentiels de ces moyens, les liaisons et les
25 interactions entre ces moyens. Une configuration
prédéterminée d'une installation permet à celle-ci
d'effectuer des traitements pour accomplir des actions
prédéterminées en vue de l'obtention d'un résultat
souhaité. Inversement, une configuration non autorisée
30 d'une installation ne permet pas à cette installation
de réaliser tout ce qui est attendu d'elle dans des
conditions souhaitées, ces conditions pouvant aller
d'un niveau de sécurité dégradé à une absence totale
de service rendu.

35

Des installations de ce type peuvent être

des ensembles complexes tels que des stations de poursuite de satellites et de traitement de signaux échangés avec ces satellites, des postes de navigation sur les navires, des automobiles équipées d'ordinateurs de bord traitant des signaux provenant par exemple de capteurs fournissant les paramètres relatifs au déplacement ou au freinage, des postes de commande de fonctionnement de centrales nucléaires, des postes de pilotage d'avions etc...

Les procédés et dispositifs de contrôle d'installations complexes doivent concourir à une plus grande sécurité de fonctionnement de ces installations grâce à une surveillance très stricte de leurs configurations.

Dans un avion par exemple, la sécurité est une préoccupation majeure des constructeurs qui adoptent de plus en plus des installations ou systèmes dits de "commande de vol électrique" incluant notamment des calculateurs, des asservissements, des capteurs etc.... Une partie importante de ces systèmes est dédiée à la surveillance et à la manoeuvre de l'avion par un ou plusieurs pilotes, à partir d'un poste central de pilotage.

Chaque installation a généralement une durée de vie importante (plusieurs années). La mise en exploitation de l'installation n'est effective qu'après des phases successives incluant notamment l'étude et la conception, la réalisation d'un prototype, la première mise en marche, les essais rendant nécessaires des modifications, puis la fabrication d'installations de série.

Les installations de série sont elles-mêmes soumises à des évolutions de configuration au cours du temps, soit pour des besoins particuliers d'un utilisateur, soit pour améliorer la qualité, la

robustesse, la fiabilité de l'installation, mais aussi pour obéir à de nouvelles réglementations ou pour utiliser de nouvelles technologies présentant de meilleures performances, ou parce que les anciennes
5 technologies sont devenues indisponibles.

Cette évolution de configuration est fréquente dans les gros avions qui sont d'autant plus concernés qu'ils sont plus modernes et mettent, par conséquent, en oeuvre un nombre plus important de
10 calculateurs. Toute évolution de configuration doit être gérée avec prudence et méthodologie, notamment pour des raisons de sécurité. Il est notamment nécessaire, lors du remplacement d'un moyen fonctionnel ancien par un nouveau moyen dans une installation,
15 de contrôler la compatibilité de ce nouveau moyen avec les autres moyens de l'installation. En effet, tout nouveau moyen fonctionnel introduit dans une installation en remplacement d'un ancien moyen ne doit pas perturber le fonctionnement de l'installation ;
20 celle-ci doit rester capable de fournir au moins les commandes fournies jusque là ou mieux, d'améliorer leur qualité.

On ne sait pas actuellement contrôler de manière automatique la validité de la configuration
25 d'une installation de traitement de données et de signaux, notamment lorsque un ou plusieurs des moyens fonctionnels combinés de cette installation sont remplacés par de nouveaux moyens.

Dans l'état actuel de la technique, pour
30 une installation comportant notamment plusieurs calculateurs recevant et échangeant des données ou des informations pour les traiter, le technicien de maintenance qui remplace un calculateur par un autre, ou modifie un programme d'un calculateur dans une
35 installation, ou remplace un capteur par un autre, modifie la configuration de celle-ci. Ce remplacement

peut intervenir par exemple lorsqu'un calculateur est en panne. Le technicien a alors le choix entre le remplacement du calculateur ancien par un calculateur identique fonctionnant avec le même programme, ou le
5 remplacement du calculateur ancien par un calculateur équivalent fonctionnant avec un programme tel que les entrées/sorties du nouveau calculateur sont identiques aux entrées/sorties de l'ancien calculateur (dans toute la suite de la description, le terme calculateur
10 désignera non seulement le matériel, mais aussi le logiciel).

Le technicien peut aussi, en respectant certaines conditions, remplacer un calculateur par un calculateur non équivalent. C'est le cas par exemple
15 lorsqu'aucun calculateur identique ou équivalent n'est disponible, ou lorsque ce remplacement est demandé par le concepteur de l'installation qui souhaite modifier la configuration de celle-ci, à la demande d'un utilisateur, ou pour améliorer la qualité du
20 fonctionnement de cette installation. La modification de configuration de l'installation, résultant par exemple du remplacement d'un calculateur par un calculateur non équivalent, exige du technicien de maintenance des procédures de vérification de la
25 cohérence du fonctionnement de l'installation. Ces procédures sont longues, compliquées, et l'erreur "humaine" dans ces vérifications est toujours un risque pouvant entraîner de graves conséquences.

Le remplacement cité en exemple est celui
30 d'un calculateur, mais ce remplacement peut être celui d'un ou plusieurs autres moyens fonctionnels de l'installation, tels que des capteurs, des circuits de mesure etc...

Le technicien de maintenance vérifie la
35 cohérence de l'installation, à partir d'informations

contenues dans un manuel de maintenance ou sur des fiches techniques.

Pour vérifier cette cohérence, il doit tout d'abord vérifier des conditions d'interchangeabilité d'un moyen existant de l'installation, par un moyen nouveau.

Il doit ensuite vérifier des conditions de compatibilité entre le moyen nouveau qui remplace un moyen existant prédéterminé et les autres moyens de l'installation avec lesquels ce moyen nouveau coopère. Tous les moyens de l'installation, ainsi qu'un moyen nouveau, sont repérés par des codes d'identification.

Les conditions d'interchangeabilité qui doivent être vérifiées sont les suivantes :

1/ Interchangeabilité simple

a) Il y a interchangeabilité simple lorsqu'un moyen existant portant un code d'identification prédéterminé est remplacé par un moyen portant le même code d'identification.

C'est par exemple le cas lorsqu'un calculateur de type et de marque prédéterminés, fonctionnant avec un programme lui-même prédéterminé, est remplacé par un calculateur de même type et de même marque, fonctionnant avec un programme identique au programme prédéterminé.

Ce cas est également celui d'un calculateur dans lequel une erreur d'exploitation apparaît au cours du déroulement du programme utilisé. Lorsque l'erreur est corrigée, c'est le code d'identification prédéterminé qui continue à être utilisé. Le moyen existant n'a en effet pas été remplacé.

b) Il y a aussi interchangeabilité simple lorsqu'un nouveau moyen, portant un nouveau code d'identification, peut remplacer le moyen existant portant un code d'identification prédéterminé.

5 C'est par exemple le cas lorsqu'un programme prédéterminé, utilisé dans un calculateur d'une installation, est remplacé par un nouveau programme capable d'exécuter les mêmes traitements que le programme existant.

10

c) Enfin, il y a aussi interchangeabilité simple lorsqu'un nouveau moyen portant un nouveau code d'identification ne peut être remplacé que par un nouveau moyen portant le même nouveau code d'identification.

15

C'est par exemple le cas lorsqu'un nouveau programme a été introduit dans un calculateur car il présente une meilleure efficacité. Ce nouveau programme ne peut être remplacé que par un programme identique, par exemple en cas d'erreur au cours du déroulement du nouveau programme. Lorsque cette erreur est corrigée, c'est le nouveau code d'identification qui continue à être utilisé.

20

25 2/ Interchangeabilité double

Il y a interchangeabilité double lorsqu'un moyen existant portant un code d'identification prédéterminé peut être remplacé par un nouveau moyen portant un nouveau code d'identification, ou réciproquement.

30

C'est par exemple le cas lorsqu'un calculateur prédéterminé, de type 286SX fonctionnant avec un programme prédéterminé (cet ensemble portant un code d'identification prédéterminé) est remplacé

35

par un calculateur de type 386SX fonctionnant avec un programme identique au programme prédéterminé. Le calculateur 386SX et son programme portent un nouveau code d'identification. Ils peuvent
5 réciproquement être remplacés par l'ancien calculateur 286SX et son programme prédéterminé portant le code d'identification prédéterminé. Dans les deux cas en effet, les entrées/sorties des calculateurs sont identiques.

10

3/ Non interchangeabilité

Un moyen ayant un code d'identification prédéterminé ou un moyen ayant un nouveau code
15 d'identification ne peuvent remplacer exclusivement qu'un moyen ayant un code d'identification identique.

C'est par exemple le cas lorsqu'un calculateur de type et de marque prédéterminés, fonctionnant avec un programme prédéterminé, ne
20 peut être remplacé que par un calculateur de même marque, de même type, et utilisant le même programme.

C'est aussi le cas lorsque la configuration d'une installation a évolué pour des raisons techniques et qu'un calculateur nouveau, utilisant
25 un nouveau programme, a remplacé un calculateur prédéterminé utilisant un programme prédéterminé. Ce nouveau calculateur et le nouveau programme ne peuvent être remplacés que par un calculateur et un programme identiques.

30

Les conditions de compatibilité qui doivent être vérifiées sont les suivantes :

35

1/ Compatibilité fonctionnelle

Lorsque dans une installation, un nouveau moyen ayant un nouveau code d'identification, remplace un moyen prédéterminé ayant un code d'identification prédéterminé, il faut s'assurer que ce nouveau moyen réalise avec une identité totale les fonctions du moyen prédéterminé. La compatibilité fonctionnelle exige que l'une des deux premières conditions d'interchangeabilité (interchangeabilité simple et interchangeabilité double) soit vérifiée.

2/ Compatibilité interne

Pour des raisons de sécurité, certaines installations comportent plusieurs voies parallèles redondantes exécutant les mêmes fonctions. Les moyens fonctionnels des différentes voies sont identiques. S'assurer de la compatibilité interne consiste à vérifier que le concepteur de l'installation autorise le remplacement d'un moyen prédéterminé dans l'une des voies, ayant un code d'identification prédéterminé, par un moyen nouveau ayant un nouveau code d'identification mais exécutant les mêmes fonctions que le moyen prédéterminé.

3/ Compatibilité externe

Cette compatibilité externe doit être vérifiée dans des installations comportant plusieurs systèmes interconnectés par des entrées et des sorties, pour échanger des données. Vérifier la compatibilité externe consiste à vérifier que le remplacement, dans l'un des systèmes, d'un moyen prédéterminé ayant un code d'identification

prédéterminé, par un moyen nouveau ayant un nouveau code d'identification, ne perturbe pas les échanges de données entre les divers systèmes de l'installation.

5

On constate bien, comme indiqué plus haut, que le contrôle de configuration d'une installation dans laquelle un ou plusieurs moyens fonctionnels sont remplacés est, pour un technicien de maintenance, un travail difficile, long, fastidieux et coûteux. De plus, le technicien peut commettre des erreurs de vérification pouvant entraîner des conséquences graves, notamment quant il s'agit d'installations de commande de vol électrique d'un avion.

15

L'invention a précisément pour but de remédier à ces inconvénients grâce à un procédé et un dispositif automatiques de contrôle de configuration d'une installation complexe. L'automaticité du procédé et du dispositif facilite notablement le travail du technicien de maintenance, permet de raccourcir notablement les délais de contrôle, et assure une très grande sécurité du contrôle de configuration d'une installation.

L'invention concerne tout d'abord un procédé de contrôle de configuration d'une installation complexe, cette installation comportant des moyens combinés présentant une configuration prédéterminée et incluant des calculateurs et des capteurs reliés à des entrées des calculateurs pour leur fournir des données et des signaux à traiter, l'installation commandant des ensembles fonctionnels reliés à des sorties des moyens combinés pour recevoir des signaux de commande, le procédé consistant à :

- affecter à chaque moyen de l'installation un code d'identification correspondant à la structure et aux spécifications fonctionnelles de ce moyen,

35

- vérifier si le remplacement d'au moins un moyen existant de l'installation auquel est attribué un code d'identification prédéterminé, par un nouveau moyen auquel est attribué un nouveau code d'identification, provoque un changement de la configuration prédéterminée de l'installation susceptible de perturber les signaux de commande fournis par l'installation, ladite vérification consistant à :

- 10 * enregistrer dans une mémoire d'un calculateur, une base des codes d'identification des moyens de l'installation, y compris le code d'identification du nouveau moyen, pour
- 15 obtenir une base de la nouvelle configuration de l'installation,
- * enregistrer dans la mémoire dudit calculateur une base de référence des codes d'identification des moyens de
- 20 l'installation, avant ledit remplacement, cette base correspondant à la configuration, dite ancienne, de l'installation,
- * comparer la base de référence des codes d'identification de l'ancienne
- 25 configuration avec la base des codes d'identification de la nouvelle configuration, pour déclencher une alarme lorsque la comparaison indique une
- 30 modification de configuration.

Selon une autre caractéristique, le procédé consiste aussi à vérifier si :

- 35 - le nouveau moyen est interchangeable avec le moyen existant,

- le nouveau moyen est interchangeable et compatible avec les autres moyens de l'installation, la base de référence contenant un dictionnaire des moyens interchangeables et compatibles.

5

Selon une autre caractéristique du procédé, celui-ci consiste à enregistrer la nouvelle configuration de l'installation dans une mémoire d'archivage du calculateur lorsque, après ladite
10 comparaison, le nouveau moyen est interchangeable et compatible avec un moyen existant qu'il remplace.

Selon une autre caractéristique, le procédé consiste ensuite à vérifier tous les critères de cas
15 de compatibilité suivants :

- compatibilité fonctionnelle,
- compatibilité interne lorsqu'un nouveau moyen remplace un moyen existant dans un ensemble de moyens redondants du système, ce nouveau moyen devant
20 être compatible avec les autres moyens redondants de l'ensemble,

- compatibilité externe lorsque les entrées et les sorties d'un système de l'installation, qui présente une nouvelle configuration, sont compatibles
25 avec les entrées et les sorties des autres systèmes de l'installation.

L'invention a aussi pour objet un dispositif de contrôle de configuration d'une installation
30 complexe, pour la mise en oeuvre du procédé, caractérisé en ce qu'il comporte un calculateur et sa mémoire, dédiés au moins au contrôle de configuration, des moyens de chargement dans la mémoire de l'ordinateur, de ladite base de référence des codes d'identification, cette
35 mémoire contenant en outre un programme de commande

d'enregistrement des codes d'identification, cette mémoire contenant en outre un programme d'enregistrement des codes d'identification des moyens de l'installation à contrôler, et un programme de comparaison de la base de référence des codes d'identification de l'ancienne configuration, et de la base des codes d'identification de la nouvelle configuration, et des moyens d'affichage reliés au calculateur, pour fournir un message d'alarme par suite d'une modification non autorisée de configuration, pour indiquer les causes de cette modification non autorisée et pour indiquer le code d'identification du nouveau moyen introduit dans l'installation et qui a provoqué cette alarme, ces moyens d'affichage fournissant aussi un message relatif à l'autorisation d'utilisation de la nouvelle configuration lorsque la comparaison n'a pas déclenché d'alarme, cette nouvelle configuration étant alors enregistrée dans lesdits moyens de changement.

Les caractéristiques et avantages de l'invention ressortiront mieux de la description qui va suivre, donnée en référence aux dessins annexés, dans lesquels :

- la figure 1 représente schématiquement et en exemple une installation complexe, contrôlée par un dispositif mettant en oeuvre le procédé de l'invention,

- la figure 2 est un organigramme qui décrit les étapes essentielles du procédé de contrôle de l'invention,

- la figure 3 est un organigramme qui décrit plus précisément les étapes relatives aux vérifications d'interchangeabilité et de compatibilité, intervenant dans l'organigramme de la figure 2.

La figure 1 représente schématiquement une installation complexe comportant par exemple deux

systèmes 1, 2 comprenant des moyens combinés permettant d'obtenir un résultat souhaité. Seul le système 1 a été représenté en détail sur la figure.

5 Ce système comporte des moyens combinés présentant une configuration prédéterminée. Dans l'exemple représenté sur la figure, le système 1 comprend des calculateurs 3, 4, 5, 6, 7, 8 et des capteurs reliés à des entrées des calculateurs. Seul l'un des capteurs 9 d'un ensemble de capteurs 10 a été représenté sur la figure.

10 Ces capteurs sont reliés à des entrées des calculateurs pour leur fournir des données et des signaux à traiter. Ces capteurs sont, par exemple pour un avion, des capteurs de vitesse, de débit de carburant, de température...etc. L'installation commande des ensembles fonctionnels 11 reliés à des sorties de calculateurs qui leurs fournissent des signaux de commande. Un ensemble fonctionnel 12 a été représenté en exemple sur la figure. Pour un avion à commandes électriques de vol, ces ensembles fonctionnels sont par exemple des asservissements.

15 Dans le système représenté en exemple sur la figure, chaque calculateur est bien entendu relié à une mémoire. Ces mémoires sont représentées en 13, 14, 15, 16, 17, 18 et elles sont respectivement reliées aux calculateurs 3, 4, 5, 6, 7, 8.

20 On a supposé que les calculateurs 6, 7, 8 forment un ensemble 19 composé de plusieurs voies redondantes, comme cela est fréquent dans un avion, pour des raisons de sécurité. En effet, toutes les voies traitent des données ou des signaux identiques et fournissent des commandes identiques, de sorte que si l'une des voies est en panne, les deux autres voies continuent à effectuer les mêmes traitements et à
30 fournir les mêmes commandes.
35

la configuration de cette installation est essentiellement représentée par les codes d'identification des moyens combinés qui la constituent (qui sont ici les calculateurs et leurs mémoires, les capteurs, les ensembles fonctionnels, les programmes enregistrés dans les mémoires...etc.), ainsi que par les liaisons d'entrée/sortie des calculateurs et des divers autres moyens. Le code d'identification de chaque calculateur peut être enregistré dans la mémoire du calculateur ou dans un registre de ce calculateur. Les codes d'identification des autres moyens de l'installation, tels que les capteurs, peuvent être des codes à barres inscrits sur des étiquettes, qui peuvent être lus par des moyens appropriés.

Le dispositif de contrôle de configuration, conforme à l'invention, comprend essentiellement, l'un des calculateurs 3 par exemple et sa mémoire 13, dédiés au contrôle de configuration de l'installation, des moyens 20 de chargement dans la mémoire 13 du calculateur dédié 3, d'une base de référence des codes d'identification des différents moyens de l'installation avant que celle-ci soit modifiée. Ces moyens d'enregistrement de la base de référence peuvent être constitués par une disquette dont le lecteur 20 est relié au calculateur dédié 3.

Le dispositif comporte aussi un ordinateur 21 avec des moyens d'affichage 25. Un clavier 26 est mis à la disposition du technicien de maintenance pour commander le lecteur de disquettes 20. Cet ordinateur est aussi relié à une mémoire 22, à une imprimante 23 et à un système 24 de lecture de codes à barres.

La mémoire 22 de l'ordinateur 21 contient notamment un programme d'enregistrement des codes d'identification des divers moyens de l'installation. Ce programme est téléchargé dans la mémoire 13 du

calculateur 3. Les codes d'identification des calculateurs de l'installation sont transmis directement au calculateur 3, par les autres calculateurs, pour être enregistrés dans la mémoire 13. Pour les autres
5 moyens, tels que les capteurs 9 par exemple, les codes d'identification sont transmis par le lecteur 24 de codes à barres.

Un programme permettant de comparer les codes d'identification des différents moyens de
10 l'installation transmis par les autres calculateurs et par le lecteur 24, et des codes d'identification de référence, est également fourni au calculateur 3 par l'ordinateur 21.

La figure 2 est un organigramme qui décrit
15 les étapes essentielles du procédé de contrôle de configuration, conforme à l'invention.

On suppose que de manière connue, chaque moyen de l'installation est affecté d'un code d'identification correspondant à la structure et aux
20 spécifications fonctionnelles de ce moyen. C'est ainsi par exemple que, pour un calculateur, le code d'identification pourra correspondre au type et à la marque du calculateur et au programme qu'il utilise.

Ces codes étant affectés, il est alors
25 nécessaire de vérifier si le remplacement d'un moyen existant, tel qu'un calculateur et/ou son programme associé, auquel est attribué un code d'identification prédéterminé, par un nouveau moyen auquel est attribué un nouveau code d'identification, ne perturbe pas la
30 cohérence du fonctionnement de l'installation et, notamment, ne perturbe pas les signaux de commande fournis par l'installation.

Cette vérification, qui consiste en fait
à contrôler la cohérence de la nouvelle configuration
35 de l'installation, est précisément obtenue de manière

automatique, à l'aide du procédé de l'invention, dont les étapes essentielles sont représentées sur la figure 2.

La première étape 101 consiste à acquérir
5 les codes d'identification des différents moyens de l'installation. Ces codes sont acquis par le calculateur dédié 3, soit directement, soit par l'intermédiaire du lecteur 24 de codes à barres.

Ils sont enregistrés dans la mémoire 13
10 de ce calculateur, à l'étape suivante 102. On suppose bien entendu que la configuration initiale et prédéterminée de l'installation a été modifiée en remplaçant un moyen existant portant un code d'identification prédéterminé, par un nouveau moyen
15 portant un nouveau code d'identification.

L'étape suivante 103 consiste à enregistrer dans la mémoire 13 du calculateur dédié 3, une base de référence des codes d'identification des moyens de l'installation, avant le remplacement de l'un au
20 moins des moyens de cette installation. Cette base est en fait un répertoire des moyens existants de l'installation, avant que sa configuration soit modifiée. La base de référence est fournie par la disquette 20, sur un ordre fourni par le technicien
25 de maintenance agissant sur le clavier de l'ordinateur 21. La base de référence est téléchargée dans la mémoire 13 du calculateur 3.

L'étape 104 consiste à comparer les codes acquis relatifs à la nouvelle configuration de
30 l'installation, après remplacement d'un ou plusieurs moyens existants, par un ou plusieurs moyens nouveaux. Cette comparaison, ainsi que les opérations de vérification qui vont suivre, sont commandées par un programme enregistré dans la mémoire 22 de l'ordinateur
35 21 et qui est téléchargé dans la mémoire 13 du calculateur 3.

L'étape 105 résulte de l'étape précédente. Elle consiste à vérifier s'il y a eu ou non changement de configuration de l'installation.

5 S'il n'y a pas eu changement de configuration, c'est que la configuration existante est validée. L'écran 25 de l'ordinateur 21 peut alors afficher un message tel que "ancienne configuration en service", comme indiqué en 106.

10 S'il y a eu changement de configuration, une alarme apparaît à l'étape 107. Cette alarme peut se traduire par un message tel que "modification de configuration", apparaissant sur l'écran de visualisation 25 de l'ordinateur 21.

15 L'apparition d'une alarme à l'étape 107 ne signifie pas obligatoirement que la nouvelle configuration n'est pas acceptable.

20 Le seul cas où la nouvelle configuration est inacceptable est celui pour lequel un moyen existant prédéterminé a été remplacé par un moyen nouveau qui n'est pas interchangeable ou est incompatible avec ce moyen existant.

25 L'étape 108 est précisément la vérification de l'interchangeabilité et de la compatibilité d'un ou plusieurs moyens de l'installation, avec les moyens existants dans la configuration initiale. A cet effet, la base de référence de codes d'identification des moyens de l'installation, avant la modification de la configuration, contient un dictionnaire des moyens interchangeables et compatibles.

30 Si dans l'installation, un moyen nouveau, portant un nouveau code d'identification, a remplacé un moyen existant, et que ce moyen nouveau n'est pas interchangeable avec le moyen existant, seule la réinstallation à l'étape 109 de l'ancien moyen ayant
35 l'ancien code d'identification prédéterminé pourra

arrêter l'alarme. Le procédé se déroule alors à nouveau de manière identique à partir de l'étape 101 et l'écran de visualisation 25 doit normalement afficher le message "ancienne configuration en service".

5 Si le moyen nouveau qui a remplacé un moyen existant est interchangeable, il est nécessaire de vérifier en plus, comme on le verra plus loin en détail à l'aide de la figure 3, la compatibilité de ce nouveau moyen avec les autres moyens de l'installation.

10 Si le moyen nouveau n'est pas compatible, seule la réinstallation du moyen existant (étape 108) portant le code d'identification prédéterminé peut permettre de valider à nouveau l'ancienne configuration, en redémarrant le procédé à l'étape 101.

15 Si le moyen nouveau portant un nouveau code d'identification, qui a remplacé un moyen existant portant un code d'identification prédéterminé, est interchangeable avec ce moyen existant, et compatible avec les autres moyens de l'installation, à la suite
20 de la vérification effectuée à l'étape 108, la nouvelle configuration est validée à l'étape 110 ; la nouvelle base des codes d'identification des moyens de la nouvelle configuration peut alors être chargée à l'étape 111, dans la disquette 20.

25 Un rapport peut être édité (étape 112) par l'imprimante 23, pour être archivé. Ce rapport indique les alarmes de modification de configuration, les résultats des vérifications d'interchangeabilité et de compatibilité, la validation d'une nouvelle
30 configuration et l'autorisation de son chargement dans la mémoire d'archivage, la disquette 20 par exemple. L'alarme est arrêtée et le message "nouvelle configuration validée" peut être affiché sur l'écran 25.

35 Le procédé peut alors en permanence redémarrer à l'étape 101.

La figure 3 est un organigramme permettant d'expliquer de manière plus détaillée l'étape 108 de vérification d'interchangeabilité et de compatibilité.

5 Cette vérification est effectuée à partir de la base des codes d'identification de moyens de la nouvelle configuration, acquis à l'étape 102, et de la base de référence des codes d'identification, téléchargée à l'étape 103, par la disquette 20. Cette vérification résulte de l'alarme apparue à l'étape 107.

La première vérification (étape 201) consiste à vérifier s'il y a interchangeabilité double. S'il n'y a pas interchangeabilité double, il est nécessaire, comme indiqué en 202, de vérifier s'il 15 y a interchangeabilité simple. S'il n'y a pas interchangeabilité simple, c'est que l'interchangeabilité est exclusive, comme indiqué en 203 et que le nouveau moyen portant un nouveau code d'identification ne peut être utilisé. La seule 20 possibilité est la réinstallation (étape 109) du moyen existant portant le code d'identification prédéterminé. Cette impossibilité d'interchangeabilité est signalée sur le rapport 112.

25 Les cas d'interchangeabilité simple, double ou exclusive ont été définis plus haut.

En cas d'interchangeabilité double ou simple, à la suite des étapes 201 ou 202, il est nécessaire de vérifier la compatibilité fonctionnelle (étape 204), la compatibilité interne (étape 205) et 30 la compatibilité externe (étape 206) du nouveau moyen portant un nouveau code d'identification, avec les autres moyens de l'installation. Les définitions de ces divers types de compatibilité ont été données plus haut.

35

20.

Si une incompatibilité quelconque apparaît, alors un rapport est édité (étape 112) et seule la réinstallation, à la place du moyen nouveau, du moyen existant avant la modification de configuration peut être envisagée (étape 109).

Si au contraire, les compatibilités fonctionnelles interne et externe sont validées, c'est que la nouvelle configuration peut elle-même être validée (étape 110).

La vérification de compatibilité interne peut être rendue nécessaire, dans l'installation représentée sur la figure 1, par exemple en cas de remplacement de l'un des calculateurs de l'ensemble des voies redondantes 19.

La vérification de la compatibilité externe peut être rendue nécessaire par exemple lorsqu'un calculateur du système 1 de l'installation est remplacé. Ce remplacement doit être compatible notamment avec les échanges de données en entrées et en sorties, entre le système 1 et le système 2.

L'invention permet bien d'atteindre les buts mentionnés plus haut, et notamment d'automatiser et d'améliorer la sécurité du contrôle de configuration d'une installation qui subit des modifications.

25

30

35

REVENDICATIONS

1. Procédé de contrôle de configuration d'une installation complexe, cette installation comportant au moins un système (1 ou 2) comprenant
- 5 des moyens combinés présentant une configuration prédéterminée et commandant des ensembles fonctionnels (11) reliés à des sorties des moyens combinés pour recevoir des signaux de commande, le procédé consistant à :
- 10 - affecter à chaque moyen de l'installation un code d'identification correspondant à la structure et aux spécifications fonctionnelles de ce moyen,
- vérifier si le remplacement d'au moins un moyen existant de l'installation auquel est attribué
- 15 un code d'identification prédéterminé, par un nouveau moyen auquel est attribué un nouveau code d'identification, provoque un changement de la configuration prédéterminée de l'installation susceptible de perturber les signaux de commande fournis
- 20 par l'installation,
- caractérisé en ce que ladite vérification consiste à :
- enregistrer (102) dans une mémoire (13)
- 25 d'un calculateur (3), une base des codes d'identification des moyens de l'installation, y compris le code d'identification du nouveau moyen, pour obtenir une base de la nouvelle configuration de l'installation,
- enregistrer (103) dans la mémoire (13)
- 30 dudit calculateur une base de référence des codes d'identification des moyens de l'installation, avant ledit remplacement, cette base correspondant à la configuration, dite ancienne, de l'installation,
- comparer (104) la base de référence des
- 35 codes d'identification de l'ancienne configuration avec la base des codes d'identification de la nouvelle

configuration, pour déclencher (107) une alarme lorsque la comparaison indique une modification de configuration.

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste aussi à vérifier (108) si :

- le nouveau moyen est interchangeable avec le moyen existant,

- le nouveau moyen est interchangeable et compatible avec les autres moyens de l'installation, la base de référence contenant un dictionnaire des moyens interchangeables et compatibles.

3. Procédé de contrôle selon la revendication 2, caractérisé en ce qu'il consiste à enregistrer (111) la nouvelle configuration de l'installation dans une mémoire d'archivage dudit calculateur, lorsque après ladite comparaison, le nouveau moyen est interchangeable et compatible avec un moyen existant qu'il remplace.

4. Procédé de contrôle selon la revendication 2, caractérisé en ce qu'il consiste ensuite à vérifier l'existence de cas de compatibilités suivants :

- compatibilité fonctionnelle (204),

- compatibilité interne (205) lorsqu'un nouveau moyen remplace un moyen existant dans un ensemble de moyens redondants du système, ce nouveau moyen devant être compatible avec les autres moyens redondants de l'ensemble,

- compatibilité externe (206) lorsque les entrées et les sorties d'un système de l'installation, qui présente une nouvelle configuration, doivent être compatibles avec les entrées et les sorties d'au moins un autre système de l'installation.

5. Dispositif de contrôle de configuration d'une installation complexe, pour la mise en oeuvre du procédé conforme à l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comporte

5 un calculateur (3) et sa mémoire (13), dédiés au moins au contrôle de configuration de l'installation, des moyens de chargement (20) dans la mémoire (13) de l'ordinateur (3) de ladite base de référence des codes d'identification, cette mémoire contenant en outre

10 un programme d'enregistrement des codes d'identification des moyens de l'installation à contrôler, et un programme de comparaison de la base de référence des codes d'identification de l'ancienne configuration, et de la base des codes d'identification de la nouvelle

15 configuration, et des moyens d'affichage (25) reliés au calculateur (3), pour fournir un message d'alarme par suite d'une modification non autorisée de configuration, pour indiquer les causes de cette modification non autorisée, et pour indiquer le code

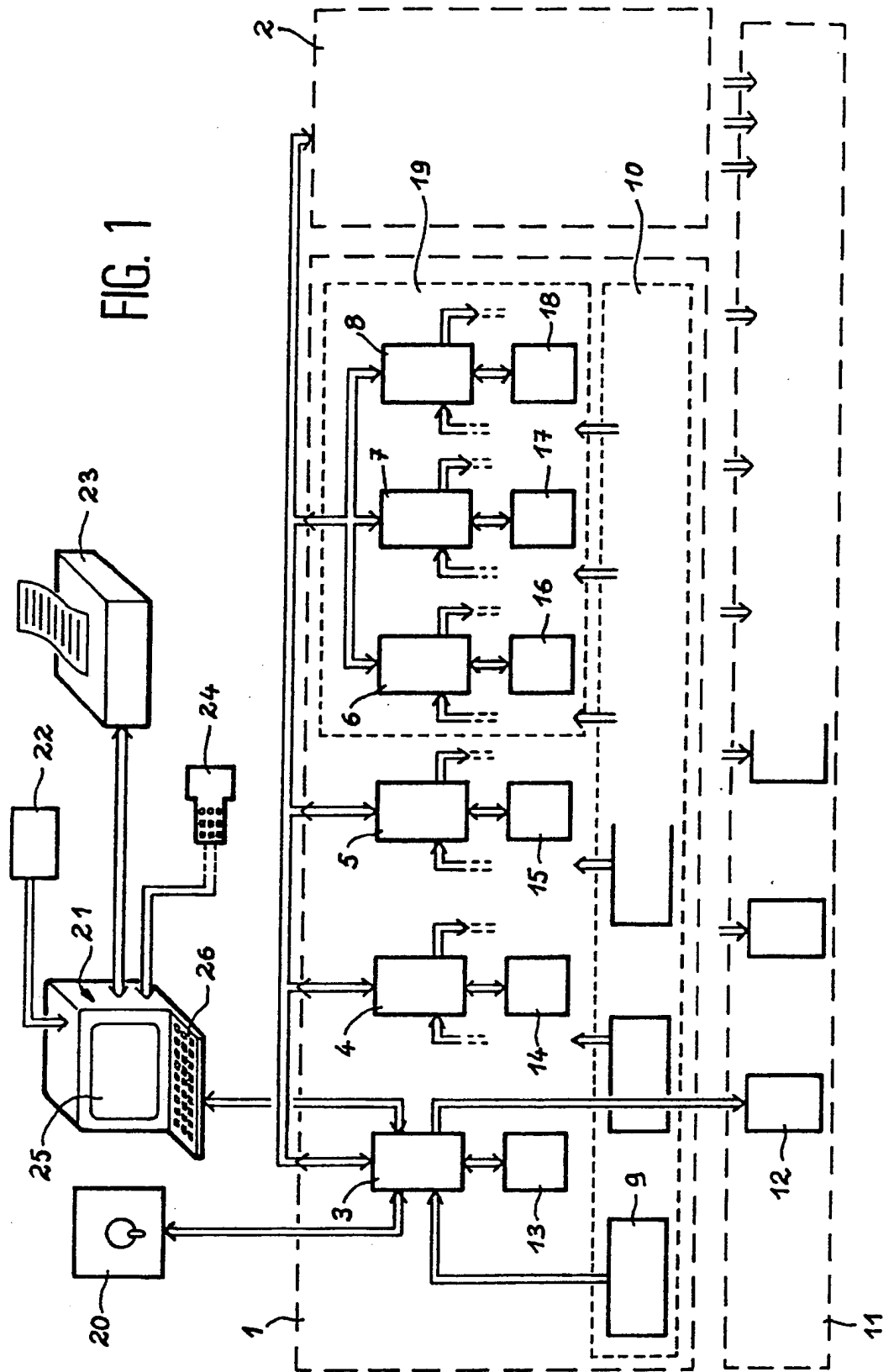
20 d'identification du nouveau moyen introduit dans l'installation et qui a provoqué cette alarme, ces moyens d'affichage fournissant aussi un message relatif à l'autorisation d'utilisation de la nouvelle configuration lorsque la comparaison n'a pas déclenché

25 d'alarme, cette nouvelle configuraion étant alors enregistrée dans lesdits moyens de chargement (20).

30

35

FIG. 1



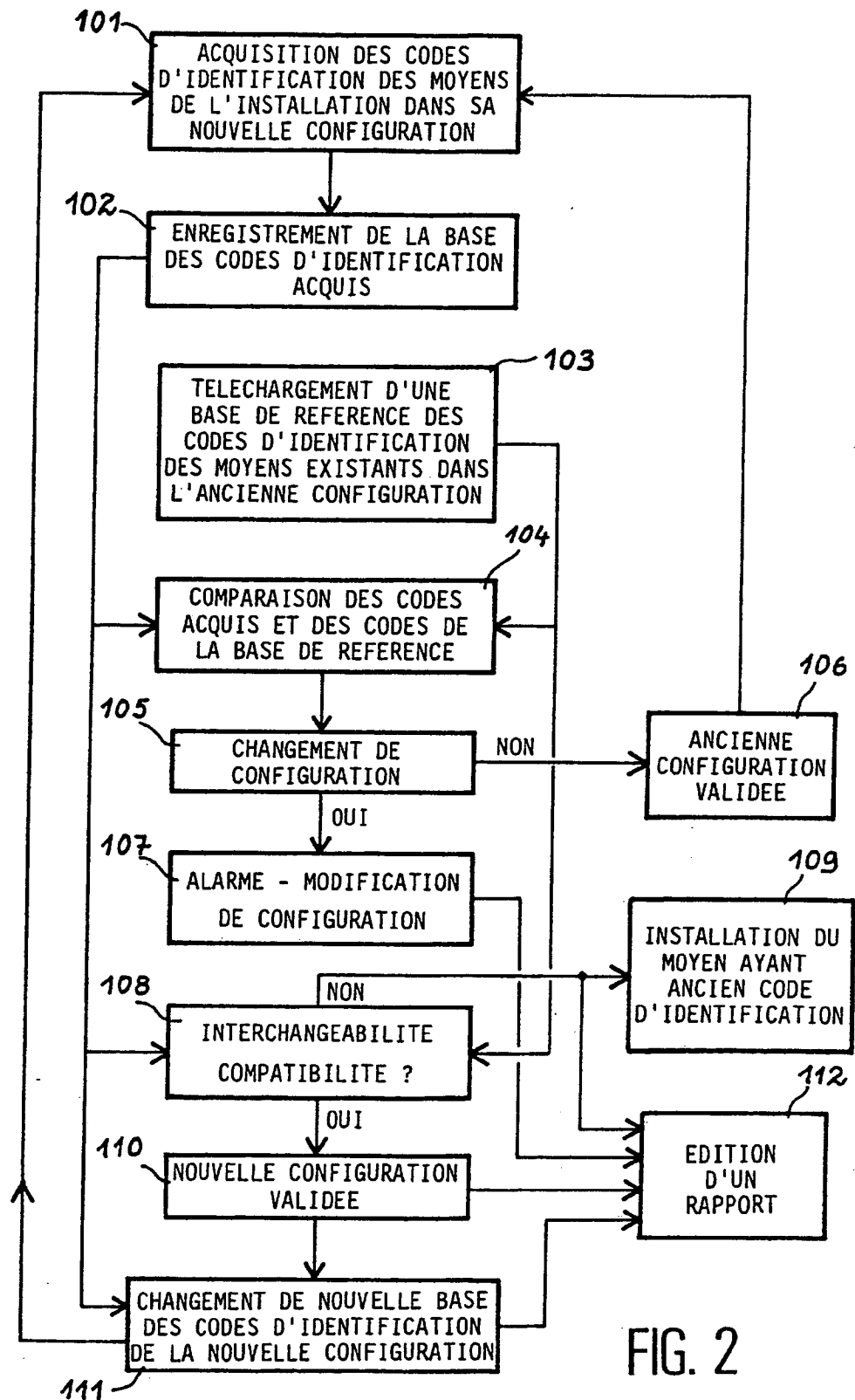
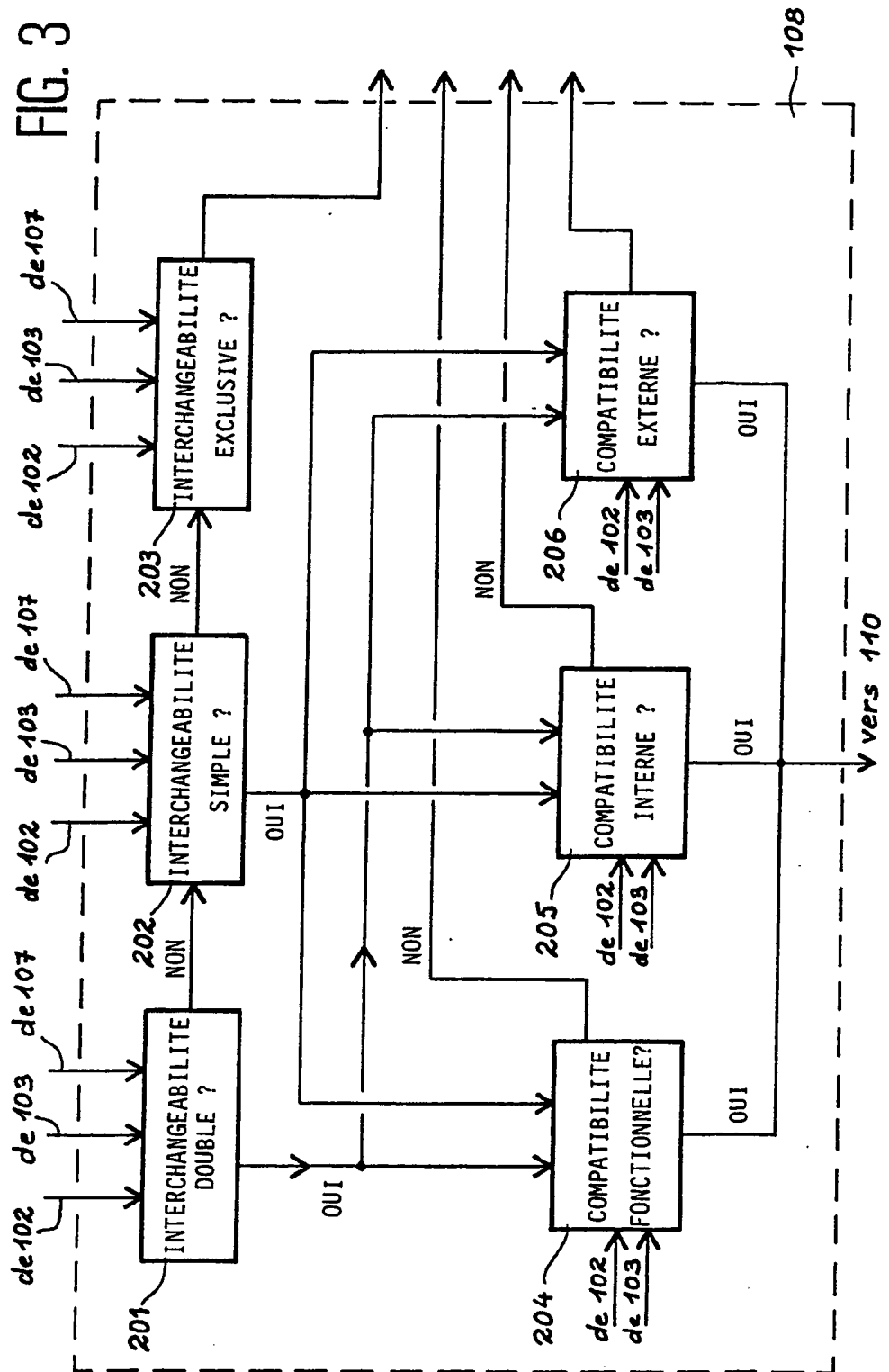


FIG. 2



INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE
établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FR 9207430
FA 476508

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	WO-A-8 912 274 (R. BOSCH) * le document en entier * ---	1-5
A	GB-A-2 203 869 (APPLE COMPUTER) * le document en entier * ---	1-5
A	GB-A-2 202 062 (THE PLESSEY COMPANY) * le document en entier * ---	1-5
A	EP-A-0 468 803 (RAYMOND CORPORATION) * le document en entier * -----	1
		DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)
		G05B G06F
Date d'achèvement de la recherche 19 FEVRIER 1993		Examinateur SOLER J.M.B.
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant</p>		